UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,897	12/18/2001	Duc Pham	AESN3005	9620

23488 7590 05/16/2005

GERALD B ROSENBERG
NEW TECH LAW
285 HAMILTON AVE
SUITE 520
PALO ALTO, CA 94301

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/016,897	PHAM ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☒ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 2 and 16 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim (Claim 1). Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 1 includes all the limitations of claim 2. The addition of the phrase "proxy" in claim 16 fails to further limit parent claim 12 as claim 12 describes the transfer of files from a repository to a client through a secure third party acting on their behalf, i.e. a proxy transfer.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-9, 12-17, 19-22, and 24-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Lin et al. (U.S. Patent No. 6,052,785)

As per claim 1, Lin discloses a network media access controller providing a centralized control point for managing secure data storage in a network-attached data

storage subsystem, said network media access controller comprising:

a) a first network interface coupleable through a first network connection to a network-attached data storage subsystem including a storage device (remote data repositories), wherein said network-attached data storage subsystem is responsive to a data storage command (request) to store first data to said storage device;

b) a second network interface coupleable through a second network connection to a client computer system, wherein said client computer system selectively provides said data storage command with respect to second data; and

c) a network data processor (server) coupled to said first network interface to provide said data storage command and first data to said second network interface to receive said data storage command and second data, said network data processor including an encryptor coupled to selectively encrypt said second data to provide said first data based on an encryption key corresponding to said storage device (CRYPTOPS) (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 2, Lin discloses the network media access controller of claim 1 wherein said encryption key is determined by said network data processor to correspond to said storage device (col.5 line 57 thru col.6 line 24).

As per claim 3, Lin discloses the network media access controller of claim 2 wherein said storage device is a logical storage unit within said network-attached storage subsystem (col.5 lines 4-13).

As per claim 4, Lin discloses the network media access controller of claim 3 wherein said network data processor includes a data table storing a plurality of encryption keys (session ids), including said encryption key, correlated against a plurality of logical storage unit identifiers (access drives), including an identifier of said logical storage unit (col.6 lines 38-59).

As per claim 5, Lin discloses the network media access controller of claim 4 wherein said data storage command includes an identification of said logical storage unit (col.3 lines 56-63).

As per claim 6, Lin discloses the network media access controller of claim 5 wherein said network data processor includes a map table storing initiator logical storage unit identifiers and target logical storage unit identifiers wherein said network access controller maps said identification provided by said data storage command through said table to select a target logical storage identifier corresponding to said logical storage unit (col.3 lines 56-63).

As per claim 7, Lin discloses a network storage access controller comprising:
a) a first network interface coupleable to an initiator network accessible by a plurality of network clients to exchange first network data, wherein said first network data contains unencrypted media-level storage data;

b) a second network interface coupleable to a target network through which a plurality of network storage volumes are accessible to exchange second network data, wherein said second network data contains encrypted media-level storage data; and

c) a controller coupled between said first and second network interfaces operative to convert between said first and second network data, said controller including a crypto processor to encrypt and decrypt media-level storage data contained in said first and second network data (CRYPTOPS) (col.3 lines 52-63; col.5 line 57 thru col.6 line 24; col.7 lines 55-57).

As per claim 8, Lin discloses the network storage access controller of claim 7 wherein said controller includes a plurality of crypto keys having predetermined association with said plurality of network storage volumes and wherein said controller is operative to selectively apply said plurality of crypto keys to convert between said first and second network data (col.3 lines 48-51;col.7 lines 48-57).

As per claim 9, Lin discloses the network storage access controller of claim 8 wherein said first and second network data includes predetermined network data packets that encapsulate media-level storage data, wherein said controller is operative to process encapsulated media-level storage data through said crypto processor selectively associated with a predetermined one of said crypto keys (col.5 line 57 thru col.6 line 23; col.7 lines 48-57).

As per claim 12, Lin discloses a network storage controller supporting client access to network attached data storage, said network controller being coupleable in a communications network between a plurality of client computers and a plurality of data stores, wherein said network storage controller provides for the transfer of network data between said client computers and said data stores, wherein said network data includes media-level data and wherein said network access controller provides for the selective encryption and decryption of said media-level data transferred with respect to said plurality of data stores (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 13, Lin discloses the network storage controller of claim 12 wherein the transfer of network data between said client computer and said data stores is directed subject to an access management policy autonomously implemented by said network storage controller (col.6 lines 25-36).

As per claim 14, Lin discloses the network storage controller of claim 13 wherein said access management policy defines a correspondence between said data stores and a plurality of encryption keys stored by said network storage controller (col.6 lines 38-49).

As per claim 15, Lin discloses the network storage controller of claim 14 wherein said access management policy defines a correspondence of data access permissions between users and said data stores (col.6 lines 38-49).

As per claim 16, Lin discloses the network storage controller of claim 12 wherein said network storage controller provides for the proxy transfer of network data between said client computers and said data stores (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 17, Lin discloses a network media access controller configures as a network proxy portal to provide storage security for clients with respect to network attached storage devices, said network media access controlled comprising a network data processor (server) coupleable between an initiator network (clients) and a target network (remote storage units) to provide for the proxy transfer of predetermined network protocol data packets containing media-level data between said initiator (client) and target (storage) networks, said network data processor being operative to selectively process said predetermined network protocol data packets to encrypt and decrypt media-level data (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 19, Lin discloses the network media access controller of claim 17 wherein said network data processor includes a plurality of encryption keys and wherein network data processor selectively processes said predetermined network protocol data packets based on a predefined correspondence between said plurality of encryption keys and a plurality of target storage resources accessible via said target network (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 20, Lin discloses the network media access controller of claim 19 wherein said predefined correspondence supports a proxy mapping of a plurality of virtual target storage devices accessible via said initiator network by a plurality of client computer systems to said plurality of target storage resources accessible via target network (col.5 lines 4-13).

As per claim 21, Lin discloses the network media access controlled of claim 20 wherein said predefined correspondence is associated with said plurality of virtual target storage devices (col.5 lines 4-13).

As per claim 22, Lin discloses the network media access controlled of claim 21 wherein said network data processor implements a data packet filter (file system gateways) to selectively provide for the proxy transfer of predetermined network protocol data packets (col.6 lines 25-36).

As per claim 24, Lin discloses a method of providing secure storage of data over a network connection, said method comprising the steps of:

a) first processing network data packets, transferred over a network between a client computer system and a storage system, to identify predetermined network data packets containing media-level data;

b) second processing said predetermined network data packets to encrypt the media-level data contained in said predetermined network data packets being transferred to said storage system and to decrypt the media-level data contained in said predetermined network data packets being transferred to said client computer system (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 25, Lin discloses the method of claim 24 wherein said storage system includes a plurality of storage resources and wherein said step of first processing determined a target storage resource from a predetermined network data packet, said method further comprising the step of selecting an encryption key corresponding to said target storage resource for use in connection with said second processing step with respect to said predetermined network data packet (col.5 line 57 thru col.6 line 23; col.7 lines 48-57).

As per claim 26, Lin discloses the method of claim 25 further comprising the step of selectively filtering (with file system gateways) network data packets permitted to be transferred over said network between said client computer system and said storage system (col.6 lines 25-36).

As per claim 27, Lin discloses the method of claim 26 further comprising the steps of:

a) providing a plurality of virtual storage resources as target storage resources for said client computer system (col.5 lines 4-13); and

b) providing a mapping of said plurality of virtual storage resources to said plurality of storage resources wherein said mapping is used in said first processing step to transfer network data packets over said network between said client computer system and said storage system (col.6 lines 25-59).

As per claim 28, Lin discloses a method of managing the secure storage of data in a network attached storage system, said method comprising the steps of:

a) establishing a network storage portal (server) through which network storage data packets are passed between a client computer system and a network data store; and

b) crypto processing, on passage through said network storage portal, media-level data contained within network storage data packets to selectively encrypt, at said network storage portal, media-level data passed to said network data store and selectively encrypt, at said network storage portal, media-level data passed from said network data store (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 29, Lin discloses the method of claim 28 wherein said network data store includes a plurality of network data store resources, said method further comprising the step of associating, at said network storage portal, media-level data encryption keys with said network data store resources to control the encryption and

decryption of media-level data passed to and from said plurality of network data store resources (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

As per claim 30, Lin discloses the method of claim 29 further comprising the step of providing, at said network storage portal, for the management of a defined key correspondence between said plurality of media-level data encryption keys and said plurality of network data store resources (col.5 line 51thru col.6 line 24).

As per claim 31, Lin discloses the method of claim 30 further comprising the steps of:

a) presenting, at said network storage portal, a plurality of virtual network data storage resources to said client computer system as targets for network storage data packets; and

b) mapping, at said network storage portal, said plurality of virtual network data store resources to said plurality of network data store resources, wherein said step of providing further provides for the management of a defined map correspondence between said plurality of virtual network data storage resources to said plurality of network data storage resources (col.6 lines 25-59).

As per claim 32, Lin discloses the method of claim 31 further comprising the step of filtering, at said network storage portal, the network storage data packets passed between said client computer system and said network data store, wherein said step of

providing further provides for the management of a filter rule set used in said filtering step to determine which network storage data packets are passed between said client computer system and said network data store (col.6 lines 25-36).

As per claim 33, Lin discloses the method claim 32 wherein said step of providing supports access by a management server to establish said defined key correspondence, said defined map, and said filter rule set (credential management system and file system gateways) (col.5 line 35 thru col.6 line 59).

As per claim 34, Lin discloses a network media access controller comprising:

a) an initiator network interface coupleable through a first network to a client initiator (client system) (col.5 lines 4-7);

b) a target network interface coupleable through a second network to a storage target (remote file system) (col.5 lines 7-13); and

c) a network data processor (server) coupled between said initiator and target network interfaces, wherein said client initiator and storage target communicate storage data over said first and second networks using a data transfer protocol (SSL/SHTTP) encapsulated by a network communications protocol (TCP/IP), wherein said data transfer protocol provides for the storage and retrieval of media-level data, wherein said network data processor (server) is operative to transfer network data packets conforming to said network communications protocol between said initiator and target network interfaces, said network data processor being further operative to selectively

encrypt an decrypt media-level data contained within network data packets transferred between said initiator and target network interfaces (CRYPTOPS) (col.3 lines 52-63; col.5 line 57 thru col.6 line 24).

Claims 1-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Berger et al. (U.S. Patent No. 5,850,446)

As per claim 1, Berger discloses a network media access controller providing a centralized control point for managing secure data storage in a network-attached data storage subsystem, said network media access controller comprising:

a) a first network interface coupleable through a first network connection to a network-attached data storage subsystem including a storage device (hosts/virtual circuits), wherein said network-attached data storage subsystem is responsive to a data storage command to store first data to said storage device;

b) a second network interface coupleable through a second network connection to a client computer system (customer/merchant computers), wherein said client computer system selectively provides said data storage command with respect to second data (col.6 line 58-col.7 line 16); and

c) a network data processor (gateway) coupled to said first network interface to provide said data storage command and first data to said second network interface to receive said data storage command (requests) and second data, said network data processor including an encryptor (encryptor/decryptor 2120) coupled to selectively encrypt said

second data to provide said first data based on an encryption key corresponding to said storage device (Abstract; Figs 21A, 22).

As per claim 2, Berger discloses the network media access controller of claim 1 wherein said encryption key is determined by said network data processor to correspond to said storage device (col.14 lines 1-26, 52-58).

As per claim 3, Berger discloses the network media access controller of claim 2 wherein said storage device is a logical storage unit within said network-attached storage subsystem (col.121 line 63 thru col.122 line 4).

As per claim 4, Berger discloses the network media access controller of claim 3 wherein said network data processor includes a data table storing a plurality of encryption keys, including said encryption key, correlated against a plurality of logical storage unit identifiers, including an identifier of said logical storage unit (col.30 lines 18-43; col.41 lines 1-50).

As per claim 5, Berger discloses the network media access controller of claim 4 wherein said data storage command includes an identification of said logical storage unit (col.17 lines 53-61).

As per claim 6, Berger discloses the network media access controller of claim 5 wherein said network data processor includes a map table storing initiator logical storage unit identifiers and target logical storage unit identifiers wherein said network access controller maps said identification provided by said data storage command through said table to select a target logical storage identifier corresponding to said logical storage unit (col.122 lines 5-50).

As per claim 7, Berger discloses a network storage access controller comprising:
a) a first network interface coupleable to an initiator network accessible by a plurality of network clients (customers/merchants) to exchange first network data, wherein said first network data contains unencrypted media-level storage data;
b) a second network interface coupleable to a target network through which a plurality of network storage volumes (hosts/virtual circuits) are accessible to exchange second network data, wherein said second network data contains encrypted media-level storage data; and
c) a controller (gateway) coupled between said first and second network interfaces operative to convert between said first and second network data, said controller including a crypto processor (2120) to encrypt and decrypt media-level storage data contained in said first and second network data (col.6 line 58-col.7 line 16; Abstract; Figs 21A, 22).

As per claim 8, Berger discloses the network storage access controller of claim 7 wherein said controller includes a plurality of crypto keys having predetermined association with said plurality of network storage volumes and wherein said controller is operative to selectively apply said plurality of crypto keys to convert between said first and second network data (col.14 lines 1-26, 52-58).

As per claim 9, Berger discloses the network storage access controller of claim 8 wherein said first and second network data includes predetermined network data packets that encapsulate media-level storage data, wherein said controller is operative to process encapsulated media-level storage data through said crypto processor selectively associated with a predetermined one of said crypto keys (col.15 lines 1-26, 52-58).

As per claim 10, Berger discloses the network storage access controller of claim 9 wherein said predetermined network data packets encapsulates SCSI protocol data (col.3 lines 31-43; col.124 lines 15-40).

As per claim 11, Berger discloses the network storage access controller of claim 10 wherein said predetermined network data packets conform to the iSCSI protocol (col.3 lines 31-43; col.124 lines 15-40).

As per claim 12, Berger discloses a network storage controller (gateway) supporting client (customer/merchant) access to network attached data storage (hosts/virtual storage), said network controller being coupleable in a communications network between a plurality of client computers and a plurality of data stores, wherein said network storage controller provides for the transfer of network data between said client computers and said data stores, wherein said network data includes media-level data and wherein said network access controller provides for the selective encryption and decryption of said media-level data transferred with respect to said plurality of data stores (col.6 line 58-col.7 line 16; Abstract; Figs 21A, 22).

As per claim 13, Berger discloses the network storage controller of claim 12 wherein the transfer of network data between said client computer and said data stores is directed subject to an access management policy autonomously implemented by said network storage controller (gateway) (col.122 lines 5-50).

As per claim 14, Berger discloses the network storage controller of claim 13 wherein said access management policy defines a correspondence between said data stores and a plurality of encryption keys stored by said network storage controller (gateway) (col.122 lines 5-50).

As per claim 15, Berger discloses the network storage controller of claim 14 wherein said access management policy defines a correspondence of data access permissions between users and said data stores (col.41 lines 1-24).

As per claim 16, Berger discloses the network storage controller of claim 12 wherein said network storage controller provides for the proxy transfer of network data between said client computers and said data stores (col.15 lines 17-21).

As per claim 17, Berger discloses a network media access controller (gateway) configured as a network proxy portal to provide storage security for clients with respect to network attached storage devices (hosts/virtual circuits), said network media access controlled comprising a network data processor coupleable between an initiator network (customers/merchants) and a target network (host/secure financial databases) to provide for the proxy transfer of predetermined network protocol data packets containing media-level data between said initiator and target networks, said network data processor being operative to selectively process said predetermined network protocol data packets to encrypt and decrypt media-level data (col.6 line 58-col.7 line 16; Abstract; Figs 21A, 22).

As per claim 18, Berger discloses the network media access controller of claim 17 wherein said predetermined network protocol data packets to conform to the iSCSI

protocol and wherein said media-level data is SCSI media data (col.3 lines 31-43; col.124 lines 15-40).

As per claim 19, Berger discloses the network media access controller of claim 17 wherein said network data processor includes a plurality of encryption keys and wherein network data processor selectively processes said predetermined network protocol data packets based on a predefined correspondence between said plurality of encryption keys and a plurality of target storage resources accessible via said target network (col.14 lines 1-26, 52-58).

As per claim 20, Berger discloses the network media access controller of claim 19 wherein said predefined correspondence supports a proxy mapping of a plurality of virtual target storage devices accessible via said initiator network by a plurality of client computer systems to said plurality of target storage resources accessible via target network (col.122 lines 5-50).

As per claim 21, Berger discloses the network media access controlled of claim 20 wherein said predefined correspondence is associated with said plurality of virtual target storage devices (col.121 lines 31-42).

As per claim 22, Berger discloses the network media access controlled of claim 21 wherein said network data processor implements a data packet filter (gateway

schemas) to selectively provide for the proxy transfer of predetermined network protocol data packets (col.15 lines 17-21).

As per claim 23, Berger discloses the network media access controller of claim 22 wherein said predetermined network protocol data packets conform to the iSCSI protocol and wherein said media-level data is SCSI media data (col.3 lines 31-43; col.124 lines 15-40).

As per claim 24, Berger discloses a method of providing secure storage of data over a network connection, said method comprising the steps of:

a) first processing network data packets, transferred over a network between a client computer system (customers/merchants) and a storage system (host), to identify predetermined network data packets containing media-level data;

b) second processing said predetermined network data packets to encrypt the media-level data contained in said predetermined network data packets being transferred to said storage system and to decrypt the media-level data contained in said predetermined network data packets being transferred to said client computer system (Abstract; col.4 lines 54-57; col.14 lines 1-26, 52-58; col.17 lines 18-30).

As per claim 25, Berger discloses the method of claim 24 wherein said storage system includes a plurality of storage resources and wherein said step of first processing determined a target storage resources from a predetermined network data

packet, said method further comprising the step of selecting an encryption key corresponding to said target storage resource for use in connection with said second processing step with respect to said predetermined network data packet (col.17 lines 53-61; col.14 lines 1-26, 52-58).

As per claim 26, Berger discloses the method of claim 25 further comprising the step of selectively filtering network data packets permitted to be transferred over said network between said client computer system and said storage system (col.4 lines 54-57).

As per claim 27, Berger discloses the method of claim 26 further comprising the steps of:

a) providing a plurality of virtual storage resources as target storage resources for said client computer system (col.121 lines 31-42); and

b) providing a mapping of said plurality of virtual storage resources to said plurality of storage resources wherein said mapping is used in said first processing step to transfer network data packets over said network between said client computer system and said storage system (col.122 lines 5-50; col.17 lines 53-61).

As per claim 28, Berger discloses a method of managing the secure storage of data in a network attached storage system, said method comprising the steps of:

a) establishing a network storage portal (gateway) through which network storage data packets are passed between a client computer system (customers/merchants) and a network data store (host/virtual circuit); and

b) crypto processing, on passage through said network storage portal, media-level data contained within network storage data packets to selectively encrypt, at said network storage portal, media-level data passed to said network data store and selectively encrypt, at said network storage portal, media-level data passed from said network data store (Abstract; col.4 lines 54-57; col.14 lines 1-26, 52-58; col.17 lines 18-30).

As per claim 29, Berger discloses the method of claim 28 wherein said network data store includes a plurality of network data store resources, said method further comprising the step of associating, at said network storage portal, media-level data encryption keys with said network data store resources to control the encryption and decryption of media-level data passed to and from said plurality of network data store resources (col.14 lines 1-26, 52-58).

As per claim 30, Berger discloses the method of claim 29 further comprising the step of providing, at said network storage portal, for the management of a defined key correspondence between said plurality of media-level data encryption keys and said plurality of network data store resources(col.14 lines 1-26, 52-58).

As per claim 31, Berger discloses the method of claim 30 further comprising the steps of:

a) presenting, at said network storage portal, a plurality of virtual network data storage resources to said client computer system as targets for network storage data packets(col.121 lines 31-42); and

b) mapping, at said network storage portal, said plurality of virtual network data store resources to said plurality of network data store resources, wherein said step of providing further provides for the management of a defined map correspondence between said plurality of virtual network data storage resources to said plurality of network data storage resources (col.122 lines 5-50; col.17 lines 53-61).

As per claim 32, Berger discloses the method of claim 31 further comprising the step of filtering, at said network storage portal, the network storage data packets passed between said client computer system and said network data store, wherein said step of providing further provides for the management of a filter rule set used in said filtering step to determine which network storage data packets are passed between said client computer system and said network data store (col.4 lines 54-57). (col.15 lines 17-21).

As per claim 33, Berger discloses the method claim 32 wherein said step of providing supports access by a management server to establish said defined key correspondence, said defined map, and said filter rule set (col.30 lines 18-43; col.41 lines 1-50; col.122 lines 5-50).

As per claim 34, Berger discloses a network media access controller comprising:

a) an initiator network interface coupleable through a first network to a client initiator (customer/merchant),

b) a target network interface coupleable through a second network to a storage target (host/virtual circuit); and

c) a network data processor coupled between said initiator and target network interfaces, wherein said client initiator and storage target communicate storage data over said first and second networks using a data transfer protocol (TCP) encapsulated by a (secure) network communications protocol, wherein said data transfer protocol provides for the storage and retrieval of media-level data, wherein said network data processor is operative to transfer network data packets conforming to said network communications protocol between said initiator and target network interfaces, said network data processor being further operative to selectively encrypt an decrypt media-level data contained within network data packets transferred between said initiator and target network interfaces (col.11 lines 44-67; col.13 lines 23-36);

As per claim 35, Berger discloses the network media access controller of claim 34 wherein said data transfer protocol is the SCSI protocol (col.3 lines 31-43; col.124 lines 15-40).

As per claim 36, Berger discloses the network media access controller of claim 35 wherein said network communications protocol is the iSCSI protocol (col.3 lines 31-43; col.124 lines 15-40).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

May 11, 2005
T.Teslovich